

## **AMENDMENTS TO THE CLAIMS**

This listing of claims will replace all prior versions, and listings, of claims in the application:

### **Listing of Claims:**

1           1. (Currently amended) A method for providing identification  
2 authentication, comprising:  
3           receiving an identification credential from an individual, including a  
4 | biometric data, wherein the identification credential is an identification card,  
5 wherein the biometric data is stored on the identification credential, and wherein  
6 the identification credential is digitally signed with a private key;  
7           receiving a biometric sample from the individual;  
8           validating the digital signature using a corresponding public key;  
9           determining if a difference between the digitally signed biometric data and  
10 the biometric sample from the individual is below a predetermined threshold; and  
11           providing the results of the determination to an interested party;  
12           whereby the identity of the individual is authenticated with reference to the  
13 identification credential alone, without having to transmit information for the  
14 individual over a network.

1           2. (Original) The method of claim 1, further comprising adjusting the  
2 predetermined threshold in accordance with instructions received from a user.

1           3. (Previously presented) The method of claim 1, wherein the  
2 identification credential includes at least one of a name, a unique ID, a citizenship,

3 an issue date, an expiration date, an identifier for an issuing authority, the  
4 biometric data, and a digital photo.

1 4. (Previously presented) The method of claim 1, wherein the biometric  
2 sample includes one of, or a combination of, a fingerprint, a signature, an iris  
3 scan, a facial scan, a voice pattern, a height, a weight, or a palm scan.

1 5. (Original) The method of claim 1, wherein the digitally signed biometric  
2 data is contained in a magnetic stripe, a bar code, a smart card, a chip-card, or a  
3 non-volatile memory, such as flash memory, located on or within the  
4 identification credential.

1 6. (Original) The method of claim 1, wherein the digital signature is  
2 provided by a central certification authority.

1 7. (Original) The method of claim 1, further comprising granting access to  
2 resources based on the determination if the difference between the digitally signed  
3 biometric data and the biometric data from the individual is below the  
4 predetermined threshold.

1 8. (Currently amended) A computer-readable storage medium storing  
2 instructions that when executed by a computer cause the computer to perform a  
3 method for providing identification authentication, the method comprising:  
4 receiving an identification credential from an individual, including a  
5 biometric data, wherein the identification credential is an identification card,  
6 wherein the biometric data is stored on the identification credential, and wherein  
7 the identification credential is digitally signed with a private key;  
8 receiving a biometric sample from the individual;

9 validating the digital signature using a corresponding public key;  
10 determining if a difference between the digitally signed biometric data and  
11 the biometric sample from the individual is below a predetermined threshold; and  
12 providing the results of the determination to an interested party;  
13 whereby the identity of the individual is authenticated with reference to the  
14 identification credential alone, without having to transmit information for the  
15 individual over a network.

1 9. (Original) The computer-readable storage medium of claim 8, wherein  
2 the method further comprises adjusting the predetermined threshold in accordance  
3 with instructions received from a user.

1 10. (Previously presented) The computer-readable storage medium of  
2 claim 8, wherein the identification credential includes at least one of a name, a  
3 unique ID, a citizenship, an issue date, an expiration date, an identifier for an  
4 issuing authority, the biometric data, and a digital photo.

1 11. (Previously presented) The computer-readable storage medium of  
2 claim 8, wherein the biometric sample includes one of, or a combination of, a  
3 fingerprint, a signature, an iris scan, a facial scan, a voice pattern, a height, a  
4 weight, or a palm scan.

1 12. (Original) The computer-readable storage medium of claim 8, wherein  
2 the digitally signed biometric data is contained in a magnetic stripe, a bar code, a  
3 smart card, a chip-card, or a non-volatile memory, such as flash memory, located  
4 on or within the identification credential.

1           13. (Original) The computer-readable storage medium of claim 8, wherein  
2           the digital signature is provided by a central certification authority.

1           14. (Original) The computer-readable storage medium of claim 8, wherein  
2           the method further comprises granting access to resources based on the  
3           determination if the difference between the digitally signed biometric data and the  
4           biometric data from the individual is below the predetermined threshold.

1           15. (Currently amended) An apparatus for providing identification  
2           authentication, comprising:

3           a receiving mechanism that is configured to receive an identification  
4           credential from an individual, including a biometric data, wherein the  
5           identification credential is an identification card, wherein the biometric data is  
6           stored on the identification credential, and wherein the identification credential is  
7           digitally signed with a private key;

8           a sampling mechanism that is configured to receive a biometric sample  
9           from the individual;

10          a validation mechanism that is configured to validate the digital signature  
11          using a corresponding public key;

12          a determination mechanism that is configured to determine if a difference  
13          between the digitally signed biometric data and the biometric sample from the  
14          individual is below a predetermined threshold; and

15          a feedback mechanism that is configured to provide the results of the  
16          determination to an interested party;

17          whereby the identity of the individual is authenticated with reference to the  
18          identification credential alone, without having to transmit information for the  
19          individual over a network.

1           16. (Original) The apparatus of claim 15, further comprising an adjustment  
2 mechanism configured to adjust the predetermined threshold in accordance with  
3 instructions received from a user.

1           17. (Previously presented) The apparatus of claim 15, wherein the  
2 identification credential includes at least one of a name, a unique ID, a citizenship,  
3 an issue date, an expiration date, an identifier for an issuing authority, the  
4 biometric data, and a digital photo.

1           18. (Previously presented) The apparatus of claim 15, wherein the  
2 biometric sample includes one of, or a combination of, a fingerprint, a signature,  
3 an iris scan, a facial scan, a voice pattern, a height, a weight, or a palm scan.

1           19. (Original) The apparatus of claim 15, wherein the digitally signed  
2 biometric data is contained in a magnetic stripe, a bar code, a smart card, a chip-  
3 card, or a non-volatile memory, such as flash memory, located on or within the  
4 identification credential.

1           20. (Original) The apparatus of claim 15, wherein the digital signature is  
2 provided by a central certification authority.

1           21. (Original) The apparatus of claim 15, further comprising a security  
2 mechanism configured to grant access to resources based on the determination if  
3 the difference between the digitally signed biometric data and the biometric data  
4 from the individual is below the predetermined threshold.